Counting subgroups of the multiplicative group

Lee Troupe
joint w/ Greg Martin

University of British Columbia

West Coast Number Theory
2017
Question from I. Shparlinski to G. Martin, circa 2009:

How many subgroups does \( \mathbb{Z}_n^\times : = (\mathbb{Z}/n\mathbb{Z})^\times \) usually have?
Question from I. Shparlinski to G. Martin, circa 2009:

How many subgroups does $\mathbb{Z}_n^\times := (\mathbb{Z}/n\mathbb{Z})^\times$ usually have?

Let $I(n)$ denote the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$. Let $G(n)$ denote the number of subsets of $\mathbb{Z}_n^\times$ which are subgroups.

Shparlinski’s question concerns the distribution of values of $I(n)$ and/or $G(n)$.

To set the stage: What do we talk about when we talk about distributions of arithmetic functions?
Average order

Let $f(n)$ be an arithmetic function.

We can ask for the average order of $f(n)$, i.e. a function $g(n)$ so that

$$\frac{1}{X} \sum_{n \leq X} f(n) \sim g(n).$$

Example: The average order of the number-of-prime-factors function $\omega(n)$ is $\log \log n$ (proof: insert the definition of $\omega(n)$, swap the order of summation, use Mertens's theorem).

This could be a starting point for studying $I(n)$ and $G(n)$, but it doesn't really answer the question.
Average order

Let $f(n)$ be an arithmetic function.
We can ask for the average order of $f(n)$, i.e. a function $g(n)$ so that

$$\frac{1}{x} \sum_{n \leq x} f(n) \sim g(n).$$

Example: The average order of the number-of-prime-factors function $\omega(n)$ is $\log \log n$ (proof: insert the definition of $\omega(n)$, swap the order of summation, use Mertens’s theorem).

This could be a starting point for studying $I(n)$ and $G(n)$, but it doesn’t really answer the question.
Normal order

We can ask for the *normal order* of \( f(n) \), i.e. a function \( g(n) \) so that, for any \( \epsilon > 0 \),

\[
\lim_{x \to \infty} \frac{1}{x} \# \left\{ n \leq x : \left| \frac{f(n)}{g(n)} - 1 \right| < \epsilon \right\} = 1.
\]
Normal order

We can ask for the normal order of $f(n)$, i.e. a function $g(n)$ so that, for any $\epsilon > 0$,

$$\lim_{x \to \infty} \frac{1}{x} \# \left\{ n \leq x : \left| \frac{f(n)}{g(n)} - 1 \right| < \epsilon \right\} = 1.$$

Theorem (Hardy, Ramanujan 1917)

The normal order of $\omega(n)$ is $\log \log n$.

Turán (1934): Proof via an upper bound for the variance (second moment) of the form

$$\frac{1}{x} \sum_{n \leq x} (\omega(n) - \log \log n)^2 \ll \log \log x.$$

We can ask for more.
The fundamental theorem of probabilistic number theory

Theorem (Erdős, Kac 1940)

Let $\omega(n)$ denote the number of distinct prime factors of a number $n$. Then

$$\lim_{x \to \infty} \frac{1}{x} \# \left\{ n \leq x : \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} < u \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} e^{-t^2/2} \, dt.$$  

In other words, the values of the function $\omega(n)$ are normally distributed, with mean and variance both equal to $\log \log n$. 

5 / 18
The fundamental theorem of probabilistic number theory

**Theorem (Erdős, Kac 1940)**

Let $\omega(n)$ denote the number of distinct prime factors of a number $n$. Then

$$
\lim_{x \to \infty} \frac{1}{x} \# \left\{ n \leq x : \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} < u \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} e^{-t^2/2} \, dt.
$$

In other words, the values of the function $\omega(n)$ are normally distributed, with mean and variance both equal to $\log \log n$.

Halberstam (1954): Proof by the method of moments, i.e. finding asymptotic formulas for each of the central moments

$$
\sum_{n \leq x} (\omega(n) - \log \log n)^k.
$$
The fundamental theorem of probabilistic number theory

Erdős and Kac’s paper establishes a normal-distribution result for a wide class of additive functions $f(n)$: $f(p_1^{e_1} \cdots p_k^{e_k}) = f(p_1^{e_1}) + \cdots + f(p_k^{e_k})$. 
The fundamental theorem of probabilistic number theory

Erdős and Kac’s paper establishes a normal-distribution result for a wide class of additive functions $f(n)$: $f(p_1^{e_1} \cdots p_k^{e_k}) = f(p_1^{e_1}) + \cdots + f(p_k^{e_k})$.

**Definition**

We say a function $f(n)$ satisfies an Erdős–Kac law with mean $\mu(n)$ and variance $\sigma^2(n)$ if

$$\lim_{x \to \infty} \frac{1}{x} \# \left\{ n \leq x : \frac{f(n) - \mu(n)}{\sigma(n)} < u \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} e^{-t^2/2} \, dt.$$
Erdős–Kac laws for non-additive functions

Theorem (Liu 2006)

For any elliptic curve \( E/\mathbb{Q} \) with CM, \( \omega(\#E(\mathbb{F}_p)) \) satisfies an Erdős–Kac law with mean and variance \( \log \log p \).

Theorem (Erdős, Pomerance 1985)

The functions \( \omega(\phi(n)) \) and \( \Omega(\phi(n)) \) both satisfy an Erdős–Kac law, with mean \( \frac{1}{2} (\log \log n)^2 \) and variance \( \frac{1}{3} (\log \log n)^3 \).

\( \Omega(\phi(n)) \) is additive; \( \omega(\phi(n)) \) isn’t!

Both are \( \phi \)-additive: If \( \phi(n) = p_{e_1} \cdots p_{e_k} \), then

\[
\omega(\phi(n)) = \omega(p_{e_1}) + \cdots + \omega(p_{e_k}).
\]
Erdős–Kac laws for non-additive functions

**Theorem (Liu 2006)**

For any elliptic curve $E/\mathbb{Q}$ with CM, $\omega(\# E(\mathbb{F}_p))$ satisfies an Erdős–Kac law with mean and variance $\log \log p$.

**Theorem (Erdős, Pomerance 1985)**

The functions $\omega(\varphi(n))$ and $\Omega(\varphi(n))$ both satisfy an Erdős–Kac law, with mean $\frac{1}{2}(\log \log n)^2$ and variance $\frac{1}{3}(\log \log n)^3$. 
Erdős–Kac laws for non-additive functions

**Theorem (Liu 2006)**

For any elliptic curve $E/\mathbb{Q}$ with CM, $\omega(\#E(\mathbb{F}_p))$ satisfies an Erdős–Kac law with mean and variance $\log \log p$.

**Theorem (Erdős, Pomerance 1985)**

The functions $\omega(\varphi(n))$ and $\Omega(\varphi(n))$ both satisfy an Erdős–Kac law, with mean $\frac{1}{2}(\log \log n)^2$ and variance $\frac{1}{3}(\log \log n)^3$.

$\Omega(\varphi(n))$ is additive;
Erdős–Kac laws for non-additive functions

**Theorem (Liu 2006)**
For any elliptic curve $E/\mathbb{Q}$ with CM, $\omega(\#E(\mathbb{F}_p))$ satisfies an Erdős–Kac law with mean and variance $\log \log p$.

**Theorem (Erdős, Pomerance 1985)**
The functions $\omega(\varphi(n))$ and $\Omega(\varphi(n))$ both satisfy an Erdős–Kac law, with mean $\frac{1}{2}(\log \log n)^2$ and variance $\frac{1}{3}(\log \log n)^3$.

$\Omega(\varphi(n))$ is additive; $\omega(\varphi(n))$ isn’t!

Both are $\varphi$-additive: If $\varphi(n) = p_1^{e_1} \cdots p_k^{e_k}$, then

$$f(\varphi(n)) = f(p_1^{e_1}) + \cdots + f(p_k^{e_k}).$$
\( \varphi \)-additivity

Recall: \( l(n) \) is the number of isomorphism classes of subgroups of \( \mathbb{Z}_n^\times \). \( G(n) \) is the number of subsets of \( \mathbb{Z}_n^\times \) which are subgroups.

Fact: Every finite abelian group is the direct product of its Sylow \( p \)-subgroups.
Recall: $I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$. $G(n)$ is the number of subsets of $\mathbb{Z}_n^\times$ which are subgroups.

Fact: Every finite abelian group is the direct product of its Sylow $p$-subgroups.

So if $G_p(n)$ denotes the number of subgroups of the Sylow $p$-subgroup of $\mathbb{Z}_n^\times$, then

$$G(n) = \prod_{p\mid \varphi(n)} G_p(n) \implies \log G(n) = \sum_{p\mid \varphi(n)} \log G_p(n)$$

and similarly for $\log I(n)$.

Thus, $\log G(n)$ and $\log I(n)$ are $\varphi$-additive functions, as well.
Erdős–Kac laws for subgroups of $\mathbb{Z}_n^\times$

Theorem (Martin–T., submitted)

The function $\log I(n)$ satisfies an Erdős–Kac law with mean

$\frac{\log 2}{2} (\log \log n)^2$ and variance $\frac{\log 2}{3} (\log \log n)^3$.

It turns out that $A \approx 0.72109$, while $\log 2 \approx 0.34657$. So, typically, $G(n) \approx I(n)^{0.089}$.9 / 18
Erdős–Kac laws for subgroups of $\mathbb{Z}_n^\times$

Theorem (Martin–T., submitted)

The function $\log I(n)$ satisfies an Erdős–Kac law with mean
$$\frac{\log 2}{2}(\log \log n)^2$$
and variance
$$\frac{\log 2}{3}(\log \log n)^3.$$  

Theorem (Martin–T., submitted)

The function $\log G(n)$ satisfies an Erdős–Kac law with mean
$$A(\log \log n)^2$$
and variance
$$C(\log \log n)^3.$$
Erdős–Kac laws for subgroups of $\mathbb{Z}_n^\times$

**Theorem (Martin–T., submitted)**

The function $\log l(n)$ satisfies an Erdős–Kac law with mean $\frac{\log 2}{2}(\log \log n)^2$ and variance $\frac{\log 2}{3}(\log \log n)^3$.

**Theorem (Martin–T., submitted)**

The function $\log G(n)$ satisfies an Erdős–Kac law with mean $A(\log \log n)^2$ and variance $C(\log \log n)^3$.

It turns out that $A \approx 0.72109$, while $\frac{\log 2}{2} \approx 0.34657$. So, typically, $G(n) \approx l(n)^{2.08}$. 
Erdős–Kac laws for subgroups of $\mathbb{Z}_n^\times$

**Theorem (Martin–T., submitted)**

The function $\log G(n)$ satisfies an Erdős–Kac law with mean $A(\log \log n)^2$ and variance $C(\log \log n)^3$.

- $A_0 = \frac{1}{4} \sum_p \frac{p^2 \log p}{(p - 1)^3(p + 1)}$

- $A = A_0 + \frac{\log 2}{2} \approx 0.72109$

- $B = \frac{1}{4} \sum_p \frac{p^3(p^4 - p^3 - p^2 - p - 1)(\log p)^2}{(p - 1)^6(p + 1)^2(p^2 + p + 1)}$

- $C = \frac{(\log 2)^2}{3} + 2A_0 \log 2 + 4A_0^2 + B \approx 3.924$
$\mathbb{Z}_n^\times$ with many subgroups

**Theorem (Martin–T., submitted)**

- The order of magnitude of the maximal order of $\log I(n)$ is $\log x / \log \log x$. More precisely,

$$
\frac{\log 2}{5} \frac{\log x}{\log \log x} \lesssim \max_{n \leq x} \log I(n) \lesssim \pi \sqrt{\frac{2}{3}} \frac{\log x}{\log \log x}.
$$

- Corollary

For any $A > 0$, there are infinitely many $n$ such that $G(n) > n^A$. 

11 / 18
Theorem (Martin–T., submitted)

- **The order of magnitude of the maximal order of** $\log I(n)$ **is** $\log x / \log \log x$. **More precisely,**

$$\frac{\log 2}{5} \frac{\log x}{\log \log x} \preceq \max_{n \leq x} \log I(n) \preceq \pi \sqrt{\frac{2}{3}} \frac{\log x}{\log \log x}.$$  

- **The order of magnitude of the maximal order of** $\log G(n)$ **is** $(\log x)^2 / \log \log x$. **More precisely,**

$$\frac{1}{16} \frac{(\log x)^2}{\log \log x} \preceq \max_{n \leq x} \log G(n) \preceq \frac{1}{4} \frac{(\log x)^2}{\log \log x}.$$
\[ \mathbb{Z}_n^\times \text{ with many subgroups} \]

**Theorem (Martin–T., submitted)**

- **The order of magnitude of the maximal order of** \( \log I(n) \) **is** \( \log x / \log \log x \). **More precisely,**

\[
\frac{\log 2}{5} \frac{\log x}{\log \log x} \lesssim \max_{n \leq x} \log I(n) \lesssim \pi \sqrt{\frac{2}{3 \log \log x}} \frac{\log x}{\log \log x}.
\]

- **The order of magnitude of the maximal order of** \( \log G(n) \) **is** \( (\log x)^2 / \log \log x \). **More precisely,**

\[
\frac{1}{16} \frac{(\log x)^2}{\log \log x} \lesssim \max_{n \leq x} \log G(n) \lesssim \frac{1}{4} \frac{(\log x)^2}{\log \log x}.
\]

**Corollary**

*For any* \( A > 0 \), *there are infinitely many* \( n \) *such that* \( G(n) > n^A \).
Proof of Erdős–Kac for $\log I(n)$

Recall: Since every subgroup of $\mathbb{Z}_n^\times$ is a direct product of subgroups of the Sylow $p$-subgroups of $\mathbb{Z}_n^\times$,

$$\log I(n) = \sum_{p \mid \varphi(n)} \log I_p(n).$$
Proof of Erdős–Kac for $\log I(n)$

Recall: Since every subgroup of $\mathbb{Z}_n^\times$ is a direct product of subgroups of the Sylow $p$-subgroups of $\mathbb{Z}_n^\times$,

$$\log I(n) = \sum_{p | \varphi(n)} \log I_p(n).$$

For all $p | \varphi(n)$, each $I_p(n)$ counts the trivial subgroup and the entire Sylow $p$-subgroup of $\mathbb{Z}_n^\times$, and so each $I_p(n) \geq 2$. So

$$\omega(\varphi(n)) \log 2 \leq \log I(n).$$
Proof of Erdős–Kac for log \(I(n)\)

For an upper bound: Write the Sylow \(p\)-subgroup of \(\mathbb{Z}_n^\times\) as

\[
\mathbb{Z}_{p^\alpha} := \mathbb{Z}_{p^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p^{\alpha_m}}
\]

for some partition \(\alpha = (\alpha_1, \ldots, \alpha_m)\) of \(\text{ord}_p(\varphi(n))\).
Proof of Erdős–Kac for log $I(n)$

For an upper bound: Write the Sylow $p$-subgroup of $\mathbb{Z}_n^\times$ as

$$\mathbb{Z}_{p^\alpha} := \mathbb{Z}_{p^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p^{\alpha_m}}$$

for some partition $\alpha = (\alpha_1, \ldots, \alpha_m)$ of $\text{ord}_p(\varphi(n))$.

There is a one-to-one correspondence between subgroups of $\mathbb{Z}_{p^\alpha}$ and subpartitions of $\alpha$. 

Now, $\#\{\text{subpartitions of } \alpha\} \leq 2^{\text{ord}_p(\varphi(n))}$.

Therefore

$$\log I(n) \leq \sum_{p|\varphi(n)} \text{ord}_p(\varphi(n)) \log 2 = \Omega(\varphi(n)) \log 2$$

$$\Rightarrow \omega(\varphi(n)) \log 2 \leq \log I(n) \leq \Omega(\varphi(n)) \log 2.$$
Proof of Erdős–Kac for $\log I(n)$

For an upper bound: Write the Sylow $p$-subgroup of $\mathbb{Z}_n^\times$ as

$$\mathbb{Z}_{p^\alpha} := \mathbb{Z}_{p^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p^{\alpha_m}}$$

for some partition $\alpha = (\alpha_1, \ldots, \alpha_m)$ of $\text{ord}_p(\varphi(n))$.

There is a one-to-one correspondence between subgroups of $\mathbb{Z}_{p^\alpha}$ and subpartitions of $\alpha$. Now,

$$\# \{ \text{subpartitions of } \alpha \} \leq 2^{\text{ord}_p(\varphi(n))}.$$
Proof of Erdős–Kac for $\log I(n)$

For an upper bound: Write the Sylow $p$-subgroup of $\mathbb{Z}_n^\times$ as

$$\mathbb{Z}_{p^\alpha} := \mathbb{Z}_{p^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p^{\alpha_m}}$$

for some partition $\alpha = (\alpha_1, \ldots, \alpha_m)$ of $\text{ord}_p(\varphi(n))$.

There is a one-to-one correspondence between subgroups of $\mathbb{Z}_{p^\alpha}$ and subpartitions of $\alpha$. Now,

$$\#\{\text{subpartitions of } \alpha\} \leq 2^{\text{ord}_p(\varphi(n))}.$$ 

Therefore

$$\log I(n) \leq \sum_{p|\varphi(n)} \text{ord}_p(\varphi(n)) \log 2 = \Omega(\varphi(n)) \log 2$$
Proof of Erdős–Kac for $\log I(n)$

For an upper bound: Write the Sylow $p$-subgroup of $\mathbb{Z}_n^\times$ as

$$\mathbb{Z}_{p^\alpha} := \mathbb{Z}_{p^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p^{\alpha_m}}$$

for some partition $\alpha = (\alpha_1, \ldots, \alpha_m)$ of $\text{ord}_p(\varphi(n))$.

There is a one-to-one correspondence between subgroups of $\mathbb{Z}_{p^\alpha}$ and subpartitions of $\alpha$. Now,

$$\#\{\text{subpartitions of } \alpha\} \leq 2^{\text{ord}_p(\varphi(n))}.$$ 

Therefore

$$\log I(n) \leq \sum_{p|\varphi(n)} \text{ord}_p(\varphi(n)) \log 2 = \Omega(\varphi(n)) \log 2$$ 

$$\implies \omega(\varphi(n)) \log 2 \leq \log I(n) \leq \Omega(\varphi(n)) \log 2.$$
What about \( \log G(n) \)?

Given a subpartition \( \beta \prec \alpha \), let \( N_p(\alpha, \beta) \) be the number of subgroups of \( \mathbb{Z}_{p^\alpha} \) isomorphic to \( \mathbb{Z}_{p^\beta} \).

**Lemma (immediate)**

\[
\log G_p(n) = \sum_{\beta \prec \alpha} \log N_p(\alpha, \beta).
\]
What about \( \log G(n) \)?

Given a subpartition \( \beta \prec \alpha \), let \( N_p(\alpha, \beta) \) be the number of subgroups of \( \mathbb{Z}_{p^\alpha} \) isomorphic to \( \mathbb{Z}_{p^\beta} \).

**Lemma (immediate)**

\[
\log G_p(n) = \sum_{\beta \prec \alpha} \log N_p(\alpha, \beta).
\]

Let \( b = (b_1, \ldots, b_{\beta_1}) \) and \( a = (a_1, \ldots, a_{\alpha_1}) \) be the partitions conjugate to \( \beta \) and \( \alpha \) respectively.
What about $\log G(n)$?

Given a subpartition $\beta \prec \alpha$, let $N_p(\alpha, \beta)$ be the number of subgroups of $\mathbb{Z}_{p^\alpha}$ isomorphic to $\mathbb{Z}_{p^\beta}$.

**Lemma (immediate)**

$$\log G_p(n) = \sum_{\beta \prec \alpha} \log N_p(\alpha, \beta).$$

Let $\mathbf{b} = (b_1, \ldots, b_{\beta_1})$ and $\mathbf{a} = (a_1, \ldots, a_{\alpha_1})$ be the partitions conjugate to $\beta$ and $\alpha$ respectively. One definition of “conjugate partition”: $a_j$ is the number of parts of $\alpha$ of size at least $j$. 
Subgroups and partitions

It turns out that

\[ N_p(\alpha, \beta) \approx \prod_{j=1}^{\alpha_1} p^{(a_j - b_j)b_j}. \]
It turns out that

\[ N_p(\alpha, \beta) \approx \prod_{j=1}^{\alpha_1} p^{(a_j-b_j)b_j}. \]

As a function of \( b_j \), the maximum of \((a_j - b_j)b_j\) occurs at \( b_j = a_j / 2 \). With this choice, \( p^{(a_j-b_j)b_j} = p^{a_j^2/4} \). These values, corresponding to the choice \( \beta = \frac{1}{2} \alpha \), provide the largest value of \( N_p(\alpha, \beta) \).
Subgroups and partitions

Lemma

For any prime $p \mid \varphi(n)$,

$$\log G_p(n) = \frac{\log p}{4} \sum_{j=0}^{\alpha_1} a_j^2 + O(\alpha_1 \log p).$$

New task: If $\mathbb{Z}_{p^\alpha}$ is the Sylow $p$-subgroup of $\mathbb{Z}_n^\times$, determine the partition $\alpha$ (or its conjugate partition $\alpha$).
Subgroups and partitions

Lemma

For any prime \( p \mid \varphi(n) \),

\[
\log G_p(n) = \frac{\log p}{4} \sum_{j=0}^{\alpha_1} a_j^2 + O(\alpha_1 \log p).
\]

New task: If \( \mathbb{Z}_{p^\alpha} \) is the Sylow \( p \)-subgroup of \( \mathbb{Z}_n^\times \), determine the partition \( \alpha \) (or its conjugate partition \( a \)).

How many of the factors in \( \mathbb{Z}_{p^\alpha} = \mathbb{Z}_{p^{\alpha_1}} \times \cdots \) are of order at least \( p^j \)?
Lemma

For any prime \( p \mid \varphi(n) \),

\[
\log G_p(n) = \frac{\log p}{4} \sum_{j=0}^{\alpha_1} a_j^2 + O(\alpha_1 \log p).
\]

New task: If \( \mathbb{Z}_{p^\alpha} \) is the Sylow \( p \)-subgroup of \( \mathbb{Z}_n^\times \), determine the partition \( \alpha \) (or its conjugate partition \( \alpha \)).

How many of the factors in \( \mathbb{Z}_{p^\alpha} = \mathbb{Z}_{p^{\alpha_1}} \times \cdots \) are of order at least \( p^j \)? We get one such factor for every prime \( q \mid n \) such that \( q \equiv 1 \pmod{p^j} \); this is the primary source of such factors.
Lemma

For any prime $p \mid \varphi(n)$,

$$\log G_p(n) = \frac{\log p}{4} \sum_{j=0}^{\alpha_1} a_j^2 + O(\alpha_1 \log p).$$

New task: If $\mathbb{Z}_{p^\alpha}$ is the Sylow $p$-subgroup of $\mathbb{Z}_n^\times$, determine the partition $\alpha$ (or its conjugate partition $a$).

How many of the factors in $\mathbb{Z}_{p^\alpha} = \mathbb{Z}_{p^{\alpha_1}} \times \cdots$ are of order at least $p^j$? We get one such factor for every prime $q \mid n$ such that $q \equiv 1 \pmod{p^j}$; this is the primary source of such factors.

So if $\omega_{p^j}(n)$ denotes the number of primes $q \mid n$, $q \equiv 1 \pmod{p^j}$, then:

$$a_j = \omega_{p^j}(n).$$

(This is exactly true if $n$ is odd and squarefree, and is true up to $O(1)$ if not.) Inserting this into the above lemma...
Sketchy in the extreme

Lemma

For any prime $p \mid \varphi(n)$,

$$\log G_p(n) = \frac{\log p}{4} \sum_{j=0}^{\alpha_1} \omega_{p^j}(n)^2 + O(\alpha_1 \log p).$$

Moreover: If $p \mid \varphi(n)$ but $p^2 \nmid \varphi(n)$, then $\log G_p(n) = \log 2$. 
Sketchy in the extreme

**Lemma**

For any prime $p \mid \varphi(n)$,

$$\log G_p(n) = \frac{\log p}{4} \sum_{j=0}^{\alpha_1} \omega_p(n)^2 + O(\alpha_1 \log p).$$

Moreover: If $p \mid \varphi(n)$ but $p^2 \nmid \varphi(n)$, then $\log G_p(n) = \log 2$.

Upon summing over all primes $p \mid \varphi(n)$:

$$\log G(n) = \sum_{p \mid \varphi(n)} \log G_p(n) \approx \log 2 \cdot \omega(\varphi(n)) + \frac{1}{4} \sum_{p^r} \omega_{p^r}(n)^2 \log p.$$
Sketchy in the extreme

Lemma

For any prime $p \mid \varphi(n)$,

\[
\log G_p(n) = \frac{\log p}{4} \sum_{j=0}^{\alpha_1} \omega_{p^j}(n)^2 + O(\alpha_1 \log p).
\]

Moreover: If $p \mid \varphi(n)$ but $p^2 \nmid \varphi(n)$, then $\log G_p(n) = \log 2$.

Upon summing over all primes $p \mid \varphi(n)$:

\[
\log G(n) = \sum_{p \mid \varphi(n)} \log G_p(n) \approx \log 2 \cdot \omega(\varphi(n)) + \frac{1}{4} \sum_{p^r} \omega_{p^r}(n)^2 \log p.
\]

Replace each of the arithmetic functions above by their known normal orders to get, for almost all $n$,

\[
\log G(n) \approx \frac{\log 2}{2} (\log \log n)^2 + \frac{1}{4} \sum_{p^r} \left( \frac{\log \log n}{\varphi(p^r)} \right)^2 \log p = A(\log \log n)^2.
\]
Future work

To handle $\log G(n)$, we approximated it by a sum of squares of additive functions.

In forthcoming work, we prove an Erdős–Kac law for arbitrary finite sums and products of additive functions satisfying standard conditions.

In other words, if $Q(x_1, \ldots, x_\ell) \in \mathbb{R}[x_1, \ldots, x_\ell]$ and $g_1, \ldots, g_\ell$ are “nice” additive functions, then $Q(g_1, \ldots, g_\ell)$ satisfies an Erdős–Kac law with a certain mean and variance.
Thanks!